

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

FILED
18 APR -4 PM 4:34

UNITED STATES OF AMERICA,

Plaintiff,

vs.

YANJUN XU,

a/k/a Xu Yanjun,

a/k/a Qu Hui,

a/k/a Zhang Hui,

Defendant.

CASE NO.

JUDGE

INDICTMENT

18 U.S.C. § 2

18 U.S.C. § 1831

18 U.S.C. § 1832

Forfeiture Allegation

1:18CR-43
J. BLACK

THE GRAND JURY CHARGES:

BACKGROUND

1. The defendant, YANJUN XU, a/k/a Xu Yanjun, a/k/a Qu Hui, a/k/a Zhang Hui (“XU”), is a citizen and resident of the People’s Republic of China. XU is a Deputy Division Director, Sixth Bureau of Jiangsu Province, Ministry of State Security, for the People’s Republic of China (“MSS”). MSS is the intelligence and security agency for China, and is responsible for counter-intelligence, foreign intelligence and political security. MSS has broad powers in China to conduct espionage both domestically and abroad.

2. China’s policies on intellectual property include a focus on the “re-innovation” of foreign technology. Technological advancement, including in the aerospace industry, is state-directed, and accomplished in part, by the acquisition of foreign technology through theft of industrial information.

3. One of XU’s job duties on behalf of MSS is to obtain technical information, including trade secrets, from aviation and aerospace companies in the United States and throughout Europe. XU sometimes uses the aliases “Qu Hui” and “Zhang Hui” in connection with his duties.

He has been known to attempt to conceal the true nature of his employment, by representing that he is associated with Jiangsu Science & Technology Promotion Association (“JAST”).

4. XU often communicates, travels, and exchanges information related to aviation technology with individuals at the Nanjing University of Aeronautics and Astronautics (“NUAA”), a public university located in Nanjing, China. NUAA is operated by the People’s Republic of China’s Ministry of Industry and Information Technology. NUAA is regarded as one of the top engineering universities in China and has significant influence over China’s aerospace industry. The Ministry of Industry and Information Technology of the Chinese government plays a significant role in regulating major industries and approving new industrial investments and projects in key areas including information technology, telecommunications, and national defense. NUAA is a regular collaborator with Commercial Aircraft Corporation of China (“COMAC”) and Aviation Industries of China (“AVIC”), hosting academic and commercial seminars and symposium and sponsoring research published by academics from NUAA.

5. Unindicted co-conspirator “CF” is a citizen and resident of the People’s Republic of China. CF is believed to be a Deputy Director at NUAA.

THE VICTIM COMPANY AND THE PROPRIETARY INFORMATION

6. Victim Company A has offices in the Southern District of Ohio. Victim Company A is among the world’s top aircraft engine suppliers for both commercial and military aircraft, and as a supplier engages in interstate and foreign commerce. Victim Company A has devoted substantial resources to research and development in the field of using unique materials to manufacture jet engine fan blades and fan containment structures. Victim Company A’s design and use of certain types of composite materials in fan blades and fan blade encasements provide greater engine durability, weight reduction, and lower costs. These fan blade and fan blade

encasement designs provide Victim Company A with a significant competitive advantage over others in the industry.

7. Victim Company A has spent several decades developing its fan blade and fan blade encasement systems over several generations of engines. Victim Company A has engaged in costly trial and error testing to advance its use of composite materials and fine-tuning, which lead to the most accurate results at the lowest cost. Through billions of dollars of research and development investment, Victim Company A developed a knowledge base of how to test jet engine fan blades and containment structures manufactured from composite materials. This testing, research, and development have led to a deep knowledge base that affords Victim Company A a powerful competitive advantage. During the course of Victim Company A's research and development, the company created numerous diagrams and drawings representing the types of tests it conducts and the results of such tests. These images and calculations are proprietary to Victim Company A, and in many instances reveal details of the company's research and development process that would provide an economic value to a competitor or other entity attempting to conduct research and development in the field of composite material jet engines. Release of some or all of this information to a competitor or any other entity attempting to conduct its own research and development in this field would provide a tremendous economic value, because it would enable the other entity to bypass costly and time-consuming research and development efforts and expend significantly fewer resources.

8. Victim Company A employs several layers of security to preserve and maintain confidentiality and to prevent unauthorized use or disclosure of its trade secrets. These steps were enforced to maintain its competitive advantage and to maintain the integrity of years of research

and development pertaining to Victim Company A's use of unique materials to manufacture jet engine fan blades and fan containment structures.

9. Some of the external physical security measures are:

(a) Limiting physical access to restricted portions of Victim Company A's campus; including through the use of manned, gated entrances and requiring identification and access badges; and

(b) Limiting visitor access to the Victim Company A's campus by mandating visitor sign-in and escorts.

10. Some of the internal security measures are:

(a) Requiring employees to execute non-disclosure and other confidentiality agreements that extend beyond the length of employment at Victim Company A;

(b) Recurrent training and instruction for employees regarding the processes in place to safeguard restricted and confidential business information;

(c) Notifying all employees that publication and/or disclosure of restricted or confidential company information is prohibited without express company authorization;

(d) Use of various data security policies; and

(e) Compartmentalizing and/or limiting access to company proprietary information to employees or contractors on a need-to-know basis.

COUNT ONE
(Conspiracy to Commit Economic Espionage)
18 U.S.C. § 1831(a)(5)

11. Paragraphs 1 through 10 are restated and re-alleged as if fully set forth herein.

12. From in or about 2013 and continuing to at least April 1, 2018, in the Southern District of Ohio and elsewhere, the defendant,

YANJUN XU,
a/k/a Xu Yanjun,
a/k/a Qu Hui,
a/k/a Zhang Hui,

and co-conspirator CF, with others known and unknown to the Grand Jury, did knowingly combine, conspire, confederate, and agree, intending and knowing that the offense will benefit a foreign government, foreign instrumentality, or foreign agent, namely **XU**, other MSS officers, NUAA, and the People's Republic of China, to:

(a) steal, and without authorization appropriate, take, carry away, and conceal, and by fraud, artifice, and deception obtain a trade secret, in violation of Title 18, United States Code, Section 1831(a)(1);

(b) without authorization, copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, and convey a trade secret, in violation of Title 18, United States Code, Section 1831(a)(2); and

(c) receive, buy, and possess a trade secret, knowing the same to have been stolen and appropriated, obtained, and converted without authorization, in violation of Title 18, United States Code, Section 1831(a)(3).

Manner and Means

13. The manner and means by which the defendant and his co-conspirators sought to accomplish the objects of the conspiracy included, among others, the following:

(a) It was part of the conspiracy that defendant **XU** and others, including other MSS officers, worked together to identify certain aviation technology that was desired by the Chinese government and associated aviation entities and universities.

(b) It was part of the conspiracy that defendant **XU** and others actively selected and targeted companies that are leaders in the field of aviation technology in the United States, including in the Southern District of Ohio, and around the world.

(c) It was further part of the conspiracy that defendant **XU** and others, including unindicted co-conspirator CF, identified engineers and experts (co-optees) who were employed by non-Chinese aviation companies and who possessed technical expertise in the desired aviation fields.

(d) It was further part of the conspiracy that defendant **XU** and others, including other MSS officers, concealed their true identities and nature of employment. Defendant **XU** and others used aliases and purported to be associated with various Chinese universities, organizations and associations, in an effort to conceal their true identities and employment with the MSS.

(e) It was further part of the conspiracy that defendant **XU** and others, including unindicted co-conspirator CF, would communicate with these co-optees, and with each other, through various messaging applications – often using their aliases and other types of false identifying information while doing so.

(f) It was further part of the conspiracy that defendant **XU** and others, including other MSS officers, would communicate and exchange messages regarding the types of

information that they wanted to obtain, and the methods they should use for obtaining the desired information.

(g) It was further part of the conspiracy that defendant **XU** and others, including other MSS officers, would communicate about the best ways to protect and conceal the true nature of the information they were seeking from aviation companies and employees, including the use of codes and series of letters in place of the technology being discussed and the name of the company being targeted.

(h) It was further part of the conspiracy that defendant **XU** and others solicited, recruited, and paid such experts to provide technical information regarding aviation technology, including trade secret information. At times, **XU** and others, including other MSS officers, accomplished this by targeting and recruiting co-optees to travel to China under the guise or false belief that the expert was traveling to China merely for “an exchange” of ideas and/or to give a presentation at a university, such as NUAA. In reality, the presentations were for the benefit of the Chinese government.

(i) It was further part of the conspiracy that defendant **XU**, and others, including unindicted co-conspirator CF, would pay the co-optees stipends and would arrange travel for and pay expenses associated with the travel to China.

(j) It was further part of the conspiracy that defendant **XU** and others would analyze the stolen technological information with experts and determine what additional technology was needed.

(k) It was further part of the conspiracy that such stolen trade secret information would be provided to the Chinese government, as well as to associated academic and commercial aviation entities, to the detriment of the owner of the trade secrets.

Overt Acts

14. In furtherance of the conspiracy and to achieve the objects and purposes thereof, defendant **XU** and others committed and caused to be committed the following overt acts, among others, in the Southern District of Ohio and elsewhere:

(a) On or about December 26, 2013, **XU** discussed an upcoming expert “exchange” with a MSS colleague. Within the messages, **XU** stated that the “customer doesn’t know our identities. I approached him with the identity of Qu Hui, the Deputy Secretary-General of Science and Technology Association.” **XU**’s colleague acknowledged, stating, “Got it. I will make sure everybody here knows you are from Nanjing Science and Technology Association.”

(b) On or about April 22, 2014, **XU** sent a message to an MSS colleague regarding another upcoming “exchange” with an expert. **XU** reminded the colleague of two things: “1. The expert does not know my true identity, I approached him with the name under Jiangsu Science and Technology Association; 2. Do not mention about the materials.”

(c) Beginning in at least March 2017, unindicted co-conspirator CF began corresponding via email with an individual (“Employee 1”) employed by Victim Company A as an engineer since 2012. Unindicted co-conspirator CF solicited Employee 1 to come to NUAA in China for an “exchange” based on Employee 1’s engineering experience at Victim Company A. NUAA, through unindicted co-conspirator CF, offered to pay for Employee 1’s travel expenses.

(d) On May 10, 2017, unindicted co-conspirator CF emailed Employee 1 that the “Institute of Energy and Power” had proposed that Employee 1 give a report on Victim Company A’s signature material design and manufacturing technology. Unindicted co-conspirator CF wanted Employee 1 to focus on highly-technical topics, including the latest developments in the application of Victim Company A’s signature material used in aeroengines, as well as engine structure design analysis technology and manufacturing technology development.

(e) On May 15, 2017, in preparation for the trip to China to present at NUAA, a message was sent to Employee 1 from one of **XU**'s email accounts, but the email was signed using the name of unindicted co-conspirator CF.

(f) While Employee 1 was in China, unindicted co-conspirator CF introduced Employee 1 to **XU**. During this meeting, **XU** introduced himself using his alias, **Qu Hui**, and claimed to be from JAST in China. **XU** gave a business card to Employee 1 that contained his alias, "**Qu Hui**," and contact information associated with JAST, a cover affiliation for **XU**.

(g) On June 2, 2017, at the invitation and direction of **XU** and unindicted co-conspirator CF, Employee 1 gave a presentation at NUAA in China, which included details regarding engines that were designed and produced by Victim Company A.

(h) **XU** had meals with Employee 1 both before and after the NUAA presentation.

(i) **XU** and others caused Employee 1 to be paid \$3,500 in U.S. currency for the presentation and as reimbursement for expenses incurred during Employee 1's visit to Nanjing (e.g., meals and hotel expenses).

(j) After the trip to China, **XU** continued to communicate with Employee 1. In fact, **XU** invited Employee 1 to return to NUAA the following year.

(k) On November 21, 2017, unindicted co-conspirator CF expressed an interest in having Employee 1 travel to China to exchange ideas and instruct again at NUAA. Unindicted co-conspirator CF informed Employee 1 that he had spoken with **Qu Hui (XU)** from JAST, and that **Qu Hui** would be able to help with travel expenses and handle the details of the "exchange."

(l) On or about January 8, 2018, **XU** wrote to Employee 1, "I will touch base with the scientific research department here to see what technology is desired and I will let you know what to prepare. For your end, please prepare the plane ticket and date as soon as possible."

(m) On or about January 23, 2018, **XU** wrote to Employee 1, “Okay. Try your best to collect and we can talk by then. Domestically, there is more focused [sic] on the system code.” **XU** later elaborated that the information he wanted pertained to “system specification, design process,” which is the application of research data to engine production. **XU** provided an email address for Employee 1 to use to send the requested information. When Employee 1 informed **XU** that the email may be blocked if Employee 1 used the company computer, **XU** responded, “It might be inappropriate to send directly from the company, right?”

(n) On or about February 3, 2018, **XU** caused Employee 1 to send an excerpt of presentation from Victim Company A, pertaining to “containment analysis” for a fan blade encasement. The document contained a label warning that the presentation contained proprietary information from Victim Company A.

(o) On February 4, 2018, **XU** wrote to Employee 1 and acknowledged receiving the document from Victim Company A pertaining to the “containment analysis.” **XU** stated that he wanted Employee 1 to spend time talking with the experts in China for a “more precise connection” and proposed a meeting date.

(p) In the same message, **XU** sent Employee 1 a list of technical topics pertaining to composite materials in the manufacture of fan blades and fan blade encasements that **XU**’s organization was interested in, after being sent information that contained Victim Company A’s proprietary warning label. Specifically, **XU** wrote, the “attached file is some domestic requirements that I know of, can you take a look and let me know if you are familiar with those?”

The attached list stated the following:

Regarding the current development situation and future development direction of foreign countries’ structural materials for fan rotor blades made from composite materials:

[A question followed.]

Regarding the design criteria for the foreign countries' composite material rotor fan blade, stator fan blade, and fan casing:

[A list of questions followed.]

(q) When Employee 1 directly advised **XU** that some of the posed questions involved Victim Company A's commercial secrets, **XU** replied they would discuss it when they met in person.

(r) In February 2018, **XU** also began discussing with Employee 1 the possibility of meeting in Europe during one of Employee 1's business trips.

(s) On or about February 5, 2018, **XU** asked Employee 1 to create and sort a directory of the files on Employee 1's computer relating to the files of Victim Company A. **XU** asked Employee 1 to send a copy of the file directory for Employee 1's company-issued computer. **XU** sent specific directions for how Employee 1 should sort and save such a directory.

(t) On or about February 14, 2018, **XU** caused Employee 1 to send a computer file directory from Employee 1's company-issued computer to **XU**.

(u) On February 28, 2018, **XU** requested to speak with Employee 1 by telephone. During the phone call, **XU** referred to the file directory that Employee 1 sent at **XU**'s request. **XU** told Employee 1 that "they" had looked at it and it is "pretty good stuff." **XU** asked if Employee 1 would be able to bring it with Employee 1 when Employee 1 traveled to Europe for their meeting. **XU** further stated, "the computer you will bring along is the company computer, right?" **XU** also asked if the material Employee 1 intended to bring could be exported out of the computer. When Employee 1 informed **XU** that it could be exported onto a portable hard drive, **XU** replied, "Good, good, good." **XU** asked, "So, if possible, we will look over the stuff. Can we do that?" After Employee 1 agreed to **XU**'s request, **XU** stated, "Do you understand? Carry the stuff along."

(v) Later in the conversation on February 28, 2018, XU told Employee 1 that what Employee 1 had sent so far was “good enough.” XU continued: “If we need something new later, we can...talk about that in person when we meet. . . What do you think? . . . All right, we really, we really don’t need to rush to do everything in one time, because, if we are going to do business together, this won’t be the last time, right?”

(w) On March 4, 2018, Employee 1 informed XU that some of the documents identified on the company directory were generated from a specific software and, as a result, some documents could only be viewed and backed up when connected to Victim Company A’s network. In response, XU asked, “Does that mean I will not be able to view these documents after I bring them back?” Employee 1 replied that Employee 1 did not know, because Employee 1 had never tried to open the files while in China.

(x) On March 5, 2018, XU sent Employee 1 a message asking, “Regarding the document directory you sent last time, is it possible to dump it to a portable hard drive or USB drive from work computer in advance?”

(y) On March 10, 2018, XU sent Employee 1 a message stating, “Since there’s still time, download more data and bring them back. Anything design related would work.”

(z) On or about April 1, 2018, XU traveled to the Kingdom of Belgium to meet Employee 1 for the purpose of discussing and receiving the sensitive information he had requested.

All in violation of Title 18, United States Code, Section 1831(a)(5).

COUNT TWO
(Conspiracy to Commit Trade Secret Theft)
18 U.S.C. § 1832(a)(5)

15. The allegations set forth in paragraphs 1 through 10 of this Indictment are incorporated herein as if set forth in full.

16. From in or about 2013 and continuing to at least April 1, 2018, in the Southern District of Ohio and elsewhere, the defendant,

YANJUN XU,
a/k/a Xu Yanjun,
a/k/a Qu Hui,
a/k/a Zhang Hui,

and co-conspirator CF, with others known and unknown to the Grand Jury, did knowingly combine, conspire, confederate and agree, with intent to convert a trade secret to the economic benefit of anyone other than the owner of the trade secret, and intending and knowing that the offense will injure any owner of that trade secret, to:

(a) steal, and without authorization appropriate, take, carry away, and conceal, and by fraud, artifice, and deception obtain such information, that is related to a product and service used in and intended for use in interstate and foreign commerce, in violation of Title 18, United States Code, Section 1832(a)(1);

(b) without authorization, copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, and convey such information, that is related to a product and service used in and intended for use in interstate and foreign commerce in violation of Title 18, United States Code, Section 1832(a)(2); and

(c) receive, buy, and possess such information, that is related to a product and service used in and intended for use in interstate and foreign commerce, knowing the same to have

been stolen and appropriated, obtained, and converted without authorization, in violation of Title 18, United States Code, Section 1832(a)(3).

Manner and Means

17. The objects of the conspiracy were carried out, in part, as alleged in paragraph 13.

Overt Acts

18. In furtherance of the conspiracy and to achieve the objects and purposes thereof, defendant XU and others committed and caused to be committed the overt acts alleged in paragraph 14, among others, in the Southern District of Ohio and elsewhere.

All in violation of Title 18, United States Code, Section 1832(a)(5).

COUNT THREE

(Attempted Economic Espionage by Theft or Fraud (Victim Company A))

18 U.S.C. §§ 1831(a)(1), 1831(a)(4) & 2

19. The allegations set forth in paragraphs 1 through 10, 13, and 14 of this Indictment are incorporated herein as if set forth in full.

20. From in or about May 2017 and continuing to at least April 1, 2018, in the Southern District of Ohio and elsewhere, the defendant,

**YANJUN XU,
a/k/a Xu Yanjun,
a/k/a Qu Hui,
a/k/a Zhang Hui,**

intending and knowing that the offense would benefit a foreign government, foreign instrumentality, or foreign agent, namely, XU, other MSS officers, NUAA, and the People's Republic of China, did knowingly attempt to steal, and without authorization attempt to appropriate, take, carry away, and conceal, and by fraud, artifice and deception attempt to obtain trade secret information owned by Victim Company A.

All in violation of Title 18, United States Code, Sections 1831(a)(1), (a)(4), and 2.

COUNT FOUR

**(Attempted Theft of Trade Secrets by Taking or Deception (Victim Company A))
18 U.S.C. §§ 1832(a)(1), 1832(a)(4) & 2**

21. The allegations set forth in paragraphs 1 through 10, 13, and 14 of this Indictment are incorporated herein as if set forth in full.

22. From in or about May 2017 and continuing to at least April 1, 2018, in the Southern District of Ohio and elsewhere, the defendant,

**YANJUN XU,
a/k/a Xu Yanjun,
a/k/a Qu Hui,
a/k/a Zhang Hui,**

with the intent to convert a trade secret to the economic benefit of someone other than Victim Company A, and intending and knowing that the offense would injure Victim Company A, did knowingly attempt to steal, and without authorization attempt to appropriate, take, carry away and conceal, and by fraud, artifice and deception attempt to obtain such information owned by Victim Company A, which was related to and included in a product and service used in and intended for use in interstate and foreign commerce.

All in violation of Title 18, United States Code, Sections 1832(a)(1), (a)(4), and 2.

FORFEITURE ALLEGATION

Upon conviction of any of the offenses set forth in Counts One through Four of this Indictment, the defendant, **YANJUN XU, a/k/a Xu Yanjun, a/k/a Qu Hui, a/k/a Zhang Hui,** shall forfeit to the United States, pursuant to 18 U.S.C. §§ 1834 and 2323, (1) any property used, or intended to be used, in any manner or part to commit or to facilitate the commission of such offenses and (2) any property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of such offenses.

SUBSTITUTE ASSETS

If any of the property described above, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,


it is the intent of the United States, pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. § 2323(b)(2)(A), to seek forfeiture of any other property of the defendant, up to the value of the property described above.

A TRUE BILL



GRAND JURY FOREPERSON

**BENJAMIN GLASSMAN
UNITED STATES ATTORNEY**



**TIMOTHY S. MANGAN
ASSISTANT UNITED STATES ATTORNEY**